UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/584,011	06/21/2006	Mario Dzeko	62630-010	4804

29493 7590 08/06/2008
HUSCH BLACKWELL SANDERS LLP
190 CARONDELET PLAZA
SUITE 600
ST. LOUIS, MO 63105-3441

EXAMINER	
WITZENBURG, BRUCE A	
ART UNIT	**PAPER NUMBER**
2166	

MAIL DATE	DELIVERY MODE
08/06/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/584,011	**Applicant(s)** DZEKO ET AL.	
	Examiner BRUCE A. WITZENBURG	**Art Unit** 2166	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 March 2008*.

2a)□ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 June 2006* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. In response to applicant's amendments filed 03/31/2008 Claims 1-15 are pending in this application.

Claim Objections

2. The following are objected to fro minor informalities:

a. In claim 8, the statement "said hash ID with modified content is not recognized by an inquiring, other person's computer" is improperly stated. The examiner suggests "said hash ID with modified content is not recognized by an inquiring (by/of) the other person's computer"

b. "the actual content" (claim 8, line 3) is objected to for lack of antecedent basis

c. In claim 9, the statement "wherein an inquiring, other person's computer" is improperly stated. The examiner suggests an inquiring, (by/of) the other person's computer.

d. "said modified content" (claim 9, lines 1-2) is objected to for lack of antecedent basis.

e. In claim 9, the statement "...is detected, searches for downloading said hash ID" is improperly stated and it is unclear who or what carries out the searches.

Claim Rejections - 35 USC § 112

3. Claim 9 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically, claim 9 leaves off information pertaining to which computer inquires and what entity within the claimed invention "searches"

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Trusted Computing, Peer-To-Peer Distribution, and the Economics of Pirated Entertainment." Stuart E Schechter, Rachel A. Greenstadt, and Michael D Smith, Hereafter Schechter, in view of "Handbook of Applied Cryptography" Alfred J Menezes, Paul C. van Oorschot and Scott A. Vanstone, hereafter "Menezes."

Regarding claim 1, Schechter discloses computers which are pooled to form an internet file sharing site which make files available in randomly stored data records, each of which including proprietary content and metadata which includes at least one hash ID (Pg 1; Pg 6, lines 31-37; Pg 7, lines 9-13) searching for the file to be protected on the internet saving at least the hash ID of each data record provided as a hit by at least one other person's computer (Pg 7, lines 20-23; Col 7, lines 38-39)

answering the inquiries from other people's computers about the file to be protected, by providing a modified data record. (Pg 7, lines 10-19 note the misrepresented data in an integrity attack provides computers asking for the information with incorrect data)

however Schechter does not disclose a method of generating a data record which is modified from the data record provided and which includes at least the saved hash ID and replacement content data linked to the saved hash ID which would work in a hashed environment.

Menezes discloses generating a data record which is modified from the data record provided and which includes at least the saved hash ID and replacement content data linked to the saved hash ID (Chapters 9.7 - 9.7.4 Note all of the above attacks are used to find data which is more or less random noise yet is indistinguishable to a hash function in order to introduce altered and corrupt data into a hashed system) Because Schechter makes it apparent that integrity attacks are well known (Pg 7, lines 10-19) and introduces a hashed system, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Schechter with the teachings of Menezes in order to produce an integrity attack which is capable of overcoming hashed systems.

Regarding claim 2, Schechter as modified discloses the step of entering and saving IP addresses of at least some of the other people's computers in the local database of one's own computer (Pg 6, lines 19-23; Pg 7, lines 10-19 Note the first scenario points out the use of IP address in recording traffic. In addition, computers must know where they're sending data to and thus must record IP addresses in some form in order to route information to its proper destination. This is made apparent by the disclosure of the network topology of Schechter) setting up a connection of one's own computer to the internet and starting the search by scanning for a search term on the other people's computer (Pg 7, lines 37-39 Note that peer-to-peer file transfer inherently entails setting up a connection to remote computers through the internet).

While Schechter does not disclose entering at least one search term identifying the file to be protected, in a local database of one's own computer it should be appreciated that a file to be modified in order to perform an integrity attack such as that which is described in Schechter, first must be located and it would have been obvious to one of ordinary skill in the art to enter search terms into an operating system's find function such as that built into Microsoft Windows 2000 and XP.

Regarding claim 3, Schechter as modified discloses one's own computer providing the modified data record belonging to the file to be protected, for downloading by the other people's computers designated by the saved IP addresses (Pg 7, lines 9-13 Note that "one's computer" in this case is equivalent to the attacker's computer and the above combined method yields an integrity attack capable of overcoming hashing functions).

Regarding claim 4, Schechter discloses the hash ID of each data record provided by another person's computer as a hit is compared with the saved hash IDs, and hits for which the result of comparison is positive are not further processed into a modified data record. (Pg 7, lines 20-24 Note that content not matching a hash is thrown out and re-downloaded)

Regarding claim 5, Schechter does not disclose the IP address of one's own computer being altered, however the DHCP protocol for determining IP address provides a method for easily setting up an internet connection which takes out IP “timeshares” which are regularly updated, and being well known in the art at the time of the invention, it would have been obvious to one of ordinary skill in the art at the time of the invention to use DHCP to establish their internet connection.

Regarding claim 6, Schechter discloses inquiries by other people's computers about the file to be protected being logged (Pg 6, lines 19-23 It should be noted that evidence for litigation includes logged traffic information and thus logging would be either inherent in the description of Schechter or obvious to one of ordinary skill in the art at the time of the invention). Schechter does not disclose logging being in anonymous form, however in order to prevent an attacker from gaining a known identity which could then be detected, it would have been obvious to one of ordinary skill in the art at the time of the invention to use identity obscuring methods to remain anonymous when gathering logging information.

Regarding claim 7, Schechter does not disclose searching for the content to be protected only being done up to a predetermined expiry date, however because the computational power of any attacker is limited, it should be appreciated that any number of metrics for determining when to cut off an attack would have been obvious to use such as number of downloaders, timestamp or date, quality rating, etc. all of which are readily available to those using file sharing sites. Because of limited computing it therefore would have been obvious to one of ordinary skill in the art to set a point based upon a known metric to cut off an attack.

Regarding claim 8, claim 8 is rejected for substantially the same reason as claim 1 above. (Note that because the hash functions are the method of detecting corrupted files, injecting content with a hash collision would not be detectable without inspecting its content.)

Regarding claim 9, claim 9 is rejected for substantially the same reason as claim 1 above.

Regarding claim 10, claim 10 is rejected for substantially the same reason as claim 2 above. (Note IP address must inherently be stored to send any information to any computer using the IP networking protocol and this would be used to carry out the above mentioned integrity attack.)

Regarding claim 11, claim 11 is rejected for substantially the same reason as claim 1 above. (Note Schechter discloses both the attacker and users on the network in his disclosure.)

Regarding claim 12, claim 12 is rejected for substantially the same reason as claim 5 above.

Regarding claim 13, claim 13 is rejected for substantially the same reason as claim 1 above. (Note the disclosed hash attacks deal exactly with replacement data.)

Regarding claim 14, claim 14 is rejected for substantially the same reason as claim 1 above. Note that the disclosure of Schechter provides hashes to deal with either the data itself or the operation of the peer to peer network and attacking a hashed file dealing with the network topology would reroute traffic.

Regarding claim 15, claim 15 is rejected for substantially the same reason as claim 14 above. Note in addition attacking a hashed file with data inside would invalidate such data.

Response to Amendment

The arguments presented by applicant are considered and deemed to be persuasive, a new grounds of rejection is presented above.

Conclusion

5. The prior art made of reference in this case is as follows:

a. "Trusted Computing, Peer-To-Peer Distribution, and the Economics of Pirated Entertainment." Stuart E Schechter, Rachel A. Greenstadt, and Michael D Smith (May 29, 2003)

b. "Handbook of Applied Cryptography" Alfred J Menezes, Paul C. van Oorschot and Scott A. Vanstone (August 1997)

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Bruce A. Witzenburg whose telephone number is 571-270-1908. The examiner can normally be reached on M-F 9:00 - 6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ali Mohammed can be reached on 571-272-4105. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

BW

/Mohammad Ali/

Supervisory Patent Examiner, Art Unit 2169